



NEW ORLEANS POLICE DEPARTMENT OPERATIONS MANUAL

CHAPTER: 41.3.9

TITLE: LICENSE PLATE RECOGNITION SYSTEM

EFFECTIVE: 01/15/2017

REVISED: Replaces Policy/Procedure 462

PURPOSE

The purpose of this Chapter is to provide officers with guidelines on the proper use of license plate recognition (LPR) systems, also commonly known as license plate reader systems.

POLICY STATEMENT

1. The availability and use of LPR systems have provided many opportunities for the enhancement of productivity, effectiveness, and officer safety. It is the policy of this agency that all members abide by the guidelines set forth herein when using LPR systems.
2. LPR systems (Fixed, Mobile and Portable) and associated equipment and databases are authorized for official public safety purposes. Misuse of this equipment and associated databases, or data, by members of the New Orleans Police Department may result in disciplinary actions.
3. LPR systems and LPR data and associated media are the property of the New Orleans Police Department and intended for use in conducting official business with limited exceptions noted elsewhere in this Chapter.

DEFINITIONS

Definitions relevant to this Chapter include:

FOUO—An acronym meaning *For Official Use Only*

LPR—License Plate Recognition / License Plate Reader

OCR—Optical Character Recognition

Read—Digital images of license plates and vehicles and associated metadata (e.g., date, time, and geographic coordinates associated with the vehicle image capture) that are captured by the LPR system.

Alert—A visual and/or auditory notice that is triggered when the LPR system receives a potential “hit” on a license plate.

Hit—A read matched to a plate that has previously been registered on an agency’s “hot list” of vehicle plates related to stolen vehicles, wanted vehicles, or other factors supporting investigation, or which has been manually registered by a user for further investigation.

Hot list—License plate numbers of stolen cars, vehicles owned by persons of interest, and vehicles associated with AMBER Alerts that are regularly added to “hot lists” circulated among law enforcement agencies. Hot list information can come from a variety of sources, including stolen vehicle information from the National Insurance Crime Bureau and the National Crime Information Center (NCIC), as well as national AMBER Alerts and Department of Homeland Security watch lists. Departments of motor vehicles can provide lists of expired registration tags, and law enforcement agencies can interface their own, locally compiled hot lists to the LPR system. These lists serve an officer safety function as well as an investigatory purpose. In addition to agency supported hot lists, users may also manually add license plate numbers to hot lists in order to be alerted if and when a vehicle license plate of interest is “read” by the LPR system. Hot lists are created to enhance law enforcement officers’ abilities to conduct investigations and provide for officer safety, the contents of hot lists are not disseminated to the public.

Fixed LPR system—LPR cameras that are permanently affixed to a structure, such as a pole, a traffic barrier, or a bridge.

Mobile LPR system—LPR cameras that are affixed, either permanently (hardwired) or temporarily (e.g., magnet-mounted), to a law enforcement vehicle for mobile deployment.

Portable LPR system—LPR cameras that are transportable and can be moved and deployed in a variety of venues as needed, such as a traffic barrel or speed radar sign.

LPR SYSTEM ADMINISTRATION - GENERAL

4. The Commander of the Special Investigations Division (SID) has administrative oversight for the LPR system (Fixed, Mobile and Portable) deployment and operation and is responsible for the following:
 - (a) Establishing protocols for access, collection, storage, and retention of LPR data and associated media files;
 - (b) Establishing protocols to preserve and document LPR reads and “alerts” or “hits” that are acted on in the field or associated with investigations or prosecutions;
 - (c) Establishing protocols to establish and ensure the security and integrity of data captured, stored, and/or retained by the LPR system;
 - (d) Selecting the personnel approved to operate the LPR system and maintaining an adequate number of trained operators;
 - (e) Maintaining records identifying approved LPR deployments and documenting their results, including appropriate documentation of significant incidents and arrests that are related to LPR usage; and
 - (f) Authorizing any requests for LPR systems use or data access according to the guidelines of this Chapter.

5. The Commander of SID, as administrator of the LPR system, should also:
 - (a) Stay abreast of legal trends and case law in the area of LPR and other electronic forms of public surveillance;
 - (b) Monitor the use of the LPR system and ensure periodic audits;
 - (c) Ensure the LPR system is only used for appropriate department business and in keeping with this Chapter;
 - (d) Manage the compilation of “hot lists”; and

- (e) Annually review and suggest necessary updates to the LPR Chapter.
6. Personnel assigned by the Commander of SID shall check LPR system equipment on a regular basis to ensure functionality and camera alignment. Any equipment that falls outside expected functionality shall be removed from service until deficiencies have been corrected.
 7. LPR system repairs, hardware or software, shall be made by Department authorized sources only.

LPR SYSTEM USAGE

8. Only members who have been properly trained in the use and operational protocols of the LPR systems shall be permitted to use it.
9. At the start of each shift authorized users must ensure that the LPR system has been updated with the most current "hot lists" available.
10. Prior to initiation of a stop based on an LPR Alert or Hit, the user (officer) must:
 - (a) Visually verify that the vehicle plate number matches the plate number run by the LPR system, including both the alphanumeric characters of the license plate and the state of issuance.
 - (b) Verify the current status of the plate through MDT query when circumstances allow.
11. **Mere receipt of an alarm is not sufficient probable cause to warrant an arrest.**
12. In each case in which an alert or a hit is triggered, the user should record the disposition of the alert and the hit into the LPR system.
13. "Hot lists" may be updated manually if the user enters a specific plate into the LPR system and wants to be alerted when that plate is located. Whenever a plate is manually entered into the LPR system, the officer shall document the reason.
14. LPR use during special or covert operations or during highly sensitive criminal investigations must be approved, in writing, by the Commander of SID. Investigations which use information obtained through the LPR database shall document the fact that LPR data was used in the investigative case report.
15. LPR reads shall not be cross-checked to obtain ownership information except for legitimate and officially sanctioned law enforcement investigations.
16. Searches of historical data within the LPR system shall be done by authorized members of SID in accordance with SID Standard Operating Guidelines (SOG's).

LPR DATA SHARING AND DISSEMINATION

17. LPR systems and associated equipment and databases are authorized FOUO (public safety purposes). Use of this equipment, associated databases, or data in a manner outside the scope of this Chapter may subject the member to disciplinary action.
18. When LPR data are disseminated **outside the Department or cooperating agencies who are sharing LPR data under existing MOU/CEA's**, it shall be documented in a Secondary Dissemination Log maintained by the Commander of SID. This log shall

clearly indicate what was shared, why it was shared, and when and who authorized the sharing.

19. Information sharing among law enforcement agencies shall be dictated in accordance with existing memoranda of understanding (MOU), cooperative endeavor agreements (CEA) or established departmental policies.

LPR SYSTEM DATA AND RECORD RETENTION

20. LPR system data, related records, logs and MOU/CEA shall be retained according to the Departmental schedule maintained by the records and Identification section of MSB. Absent specific a specific schedule, the data shall be purged after 180 days.